METHOD FOR PROVIDING LONG-LIVED BROADCAST ENCRYPTION

BACKGROUND

1. Technical Field:

The present application relates generally to broadcast encryption and, more particularly, to a long-lived broadcast encryption scheme that adapts to the presence of pirate decoders and maintains the security of broadcast to authorized users as encryption keys are compromised over time.

2. Description of Related Art:

In general, broadcast encryption (BE) techniques are employed to encrypt digital content to ensure that only privileged users are able to recover the content from an encrypted broadcast. Keys are allocated in such a way ~~hat~~ That users may be prevented on a short-term basis from recovering the message from the encrypted content. This short-term exclusion of users occurs, for example, when a proper subset of users request to view a movie. The long-term exclusion (or, revocation) of a user is necessary when a user leaves the system entirely.

In practice, broadcast encryption schemes are typically smartcard-based, wherein key material is held in a "tamper-resistant", replaceable smartcard. These smartcards, however, may be used to construct pirate smartcards (or pirate decoders) that allow non-paying customers to recover content. For instance, a coalition of unscrupulous users may conspire to attack a BE system by breaking open their smartcards to extract the keys and build pirate decoders using the extracted decryption keys, allowing non-authorized,